James Runyon

Los Lunas, NM 87031 | 505-313-2307 | James@jrunyon.tech
https://jrunyon.tech/
https://github.com/The-WatchDog
https://www.linkedin.com/in/james-runyon-8b4ab51a4

An obsessed and aspiring Cybersecurity Red teamer, boasting an impressive Kali Linux home lab and vulnerable AD environment, with 4+ years of experience managing client site security, assembling quarterly marketing progress and security incident reports, and maintaining the utmost professionalism with clients, all while having an unwavering fascination with all things CyberSec, OWASP, malware analysis, and penetration testing.

Red Team Experience

HACKING LAB – KALI LINUX   January 2021
- Built a Kali Linux hacking lab within virtual box.
- Wrote a Python script to scan ports faster.
- Dissected potential malware and used Mandiant Red Line to classify any IOC's.

HOME LAB – AD DOMAINAND VULNERABLE MACHINES   February 2022
- Built multiple windows machines to replicate a true-to-life company like Active Directory, with built in commonly found vulnerabilities to better train in AD type attacks and exploits.
- Built and installed several vulnerable machines to practice real life attacks and exploits, and master different techniques in preparation for a real pentesting job.

TRY HACK ME / HACK THE BOX   March 2022
- Fought my way to rank **19589** of all **1269151** users, placing me in the top 2% of all players, and completed **23** THM labs and rooms.
- Successfully exploited **10** rooms on Hack the Box.1

Certifications

Pentester Lab	*Unix Badge*
Security Blue Team	*Introduction to Threat Hunting*
Try Hack Me	*Pre-Security Learning Path*
Try Hack Me	*Beginner Path*
INE	*eJPT* (Junior Penetration Tester, *estimated August 16*)
Offensive Security	*OSCP* (*estimated February 2023*)

Professional Experience

AQUA VITA CREATIVE   July 2020 - Present
Content Manager
- Created personalized and curated content for our widely varying clientele (such as the Tulsa Opera and the Bama Cooperation) with a focus on bringing traffic to their various websites, increasing overall sales to meet their goals, and taking necessary steps to secure the client's site to align with industry standard.
- Scanned client sites for potential breaches/vulnerabilities weekly using industry tools such as **Nessus**, **WPScan,** and **Burpsuite.**
- Created quarterly Google Drive marketing reports based on the sales and website traffic results for that period as well as any security breaches encountered during audit, and steps taken to resolve breach or vulnerability .

Education

UNIVERSITY OF NEW MEXICO